Veille n 2 - Les bonnes pratiques de securisation d'Active Directory

Active Directory reste une cible prioritaire des cyberattaquants. Sa securisation repose sur plusieurs piliers : GPO, moindre privilege, protection des comptes admin et surveillance continue.

GPO de securite

Les GPO permettent d'appliquer des configurations de securite de facon centralisee. Microsoft (2025) recommande de bloquer les protocoles obsoletes NTLMv1 et SMBv1, d'exiger la signature LDAP, de desactiver LLMNR et d'activer Windows LAPS pour les mots de passe administrateurs locaux. Toute modification incorrecte d'un GPO pouvant avoir des consequences graves, une surveillance des changements est indispensable.

Principe du moindre privilege

Il consiste a n'accorder que les droits strictement necessaires a chaque utilisateur. En pratique : limiter les membres des groupes privilegies (Domain Admins), creer des comptes de service dedies et appliquer le Tier Model. Ce modele segmente les ressources en trois niveaux (controleurs de domaine, serveurs metier, postes de travail) pour freiner la propagation laterale d'une attaque (Semperis, janvier 2026).

Securisation des comptes administrateurs

Le MFA doit etre active sur tous les comptes a privileges. Les administrateurs doivent utiliser des postes dedies (PAW), isoles du reseau standard. Les comptes Domain Admin ne doivent jamais servir a naviguer sur Internet. Microsoft recommande egalement les politiques de mots de passe a granularite fine (FGPP) pour imposer des exigences plus strictes selon le niveau de privilege.

Surveillance et audit

La securisation d'AD est un processus continu. Il faut activer l'audit avancee pour journaliser les connexions et modifications, et utiliser des outils comme Microsoft Defender for Identity ou PingCastle pour detecter les comportements anormaux et les chemins d'attaque (Vaadata, mars 2025).

Sources

- Microsoft Learn - Meilleures pratiques pour la securisation d'Active Directory, aout 2025
- Semperis - Active Directory Security Best Practices, janvier 2026
- Vaadata - Securite Active Directory : failles et bonnes pratiques, mars 2025